Haruspex
Cyber Risk Assessment and Management

Università di Pisa

Cybersecurity: Current and Future Challenges

F. Baiardi
f.baiardi@unipi.it
Full professor, Università di Pisa &
Haruspex (Cofounder & Scientific Executive)

Whoami

- Computer science professor
- My research topic :

  quantitative assessment and management of cyber risk
- My group developed a framework to assess and manage cyber risk using digital twins of the target system and of attackers (Haruspex)
- I have coordinated several cyber risk assessments of
  - Industrial control systems
  - Power and gas distribution infrastructures
  - Smart meter infrastructures
- I have written several scientific dissemination papers

Cybersecurity

Current status

- Bad Thank you
- The good news is awareness
- The bad news is that old solutions are still in use

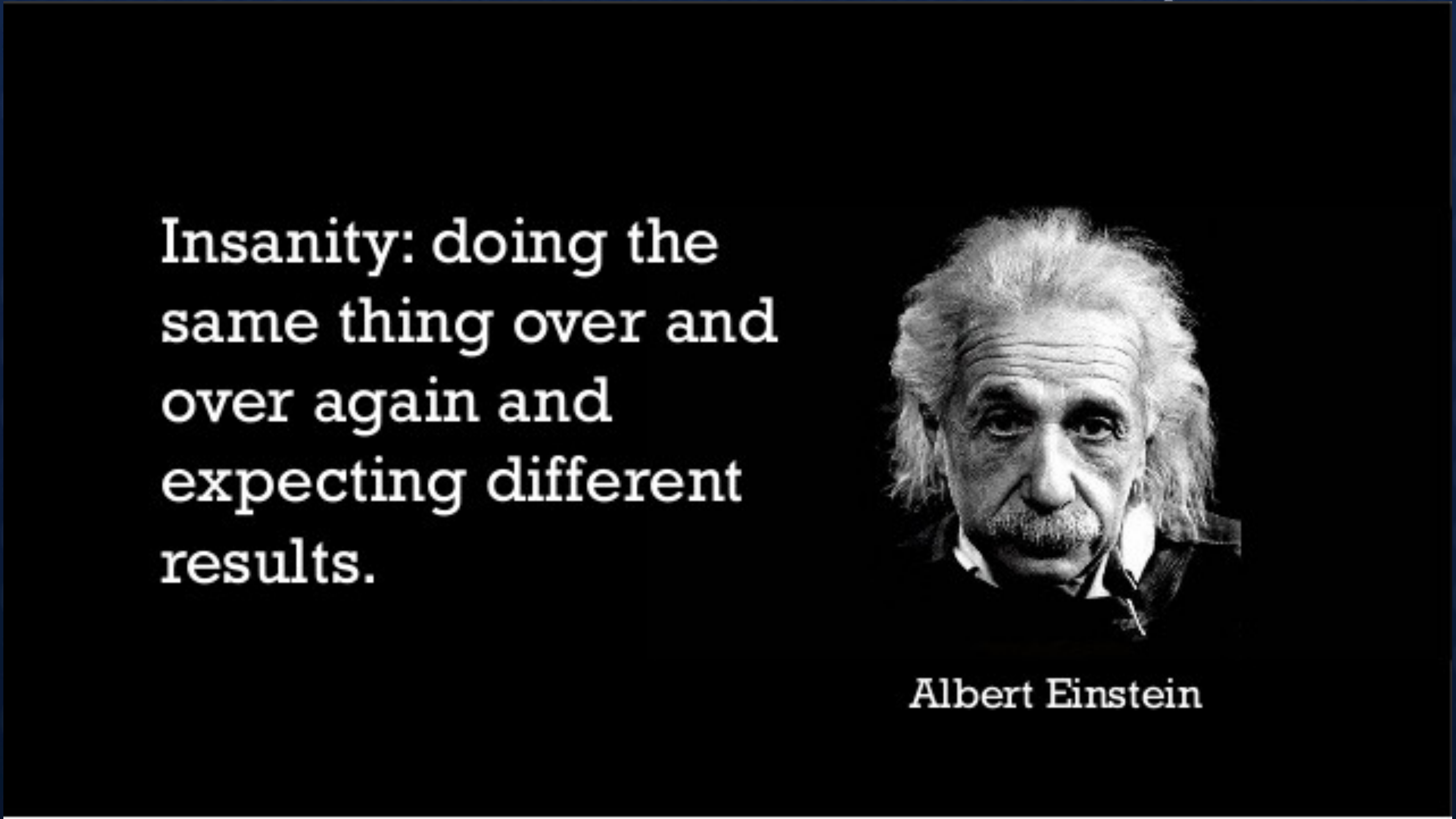
Current Challenges

- Supply chain attacks
- Ransomware

Future Challenges

- AI as a source of tools & methods
- AI vs old problems

Cybersecurity current status

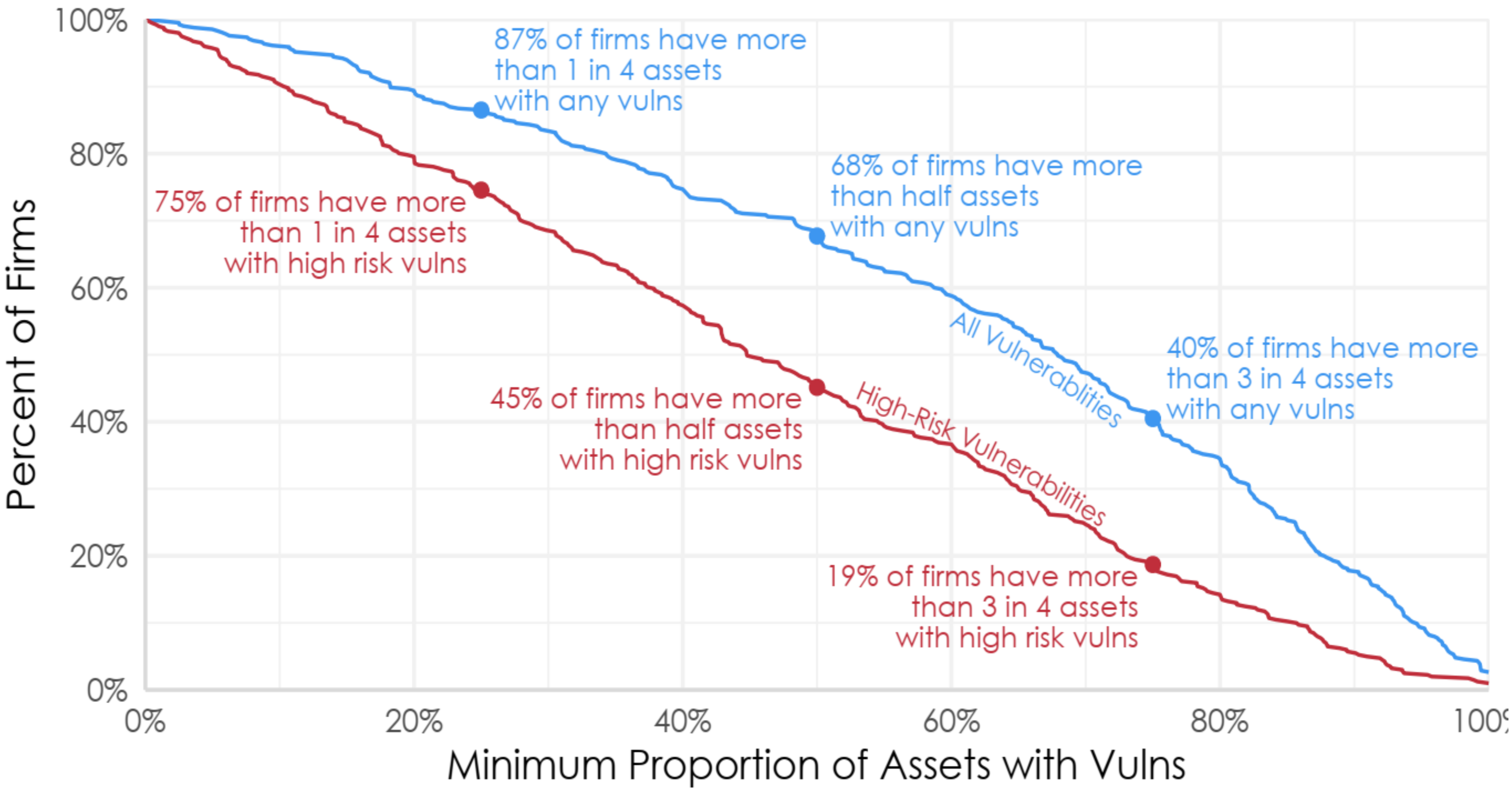


Insanity: doing the same thing over and over again and expecting different results.

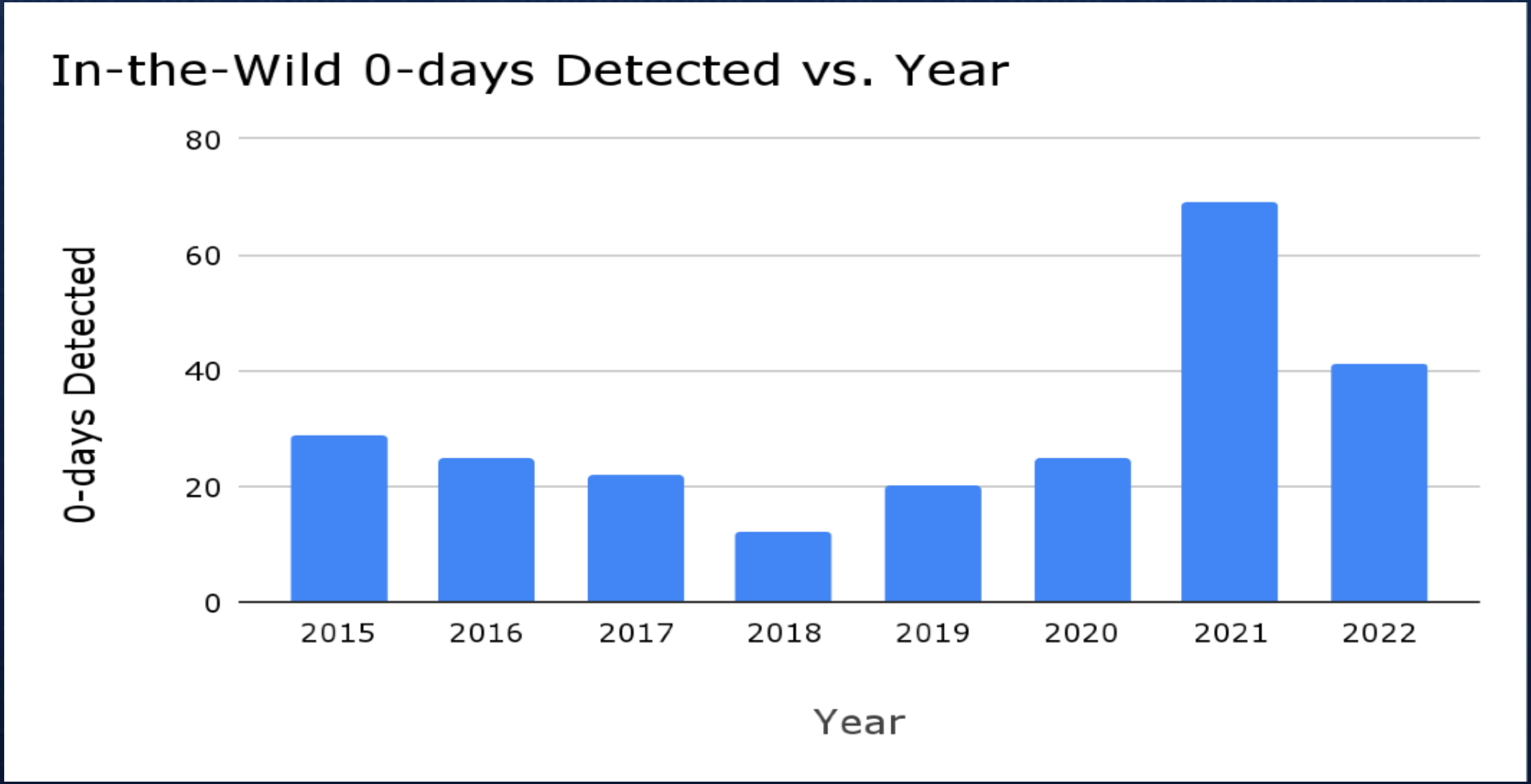
Albert Einstein

(true even if is a misquotation)

Why attackers are successful

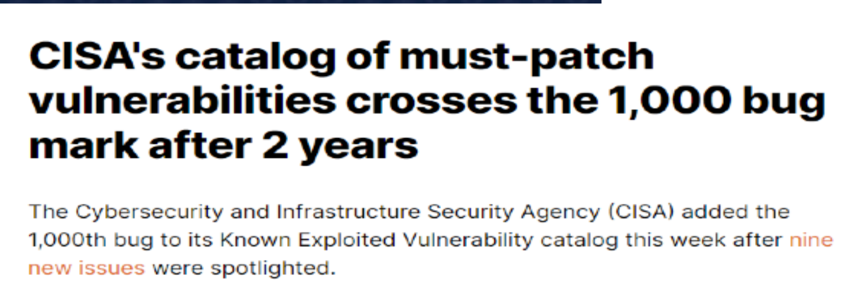


Zero days no longer reserved to states



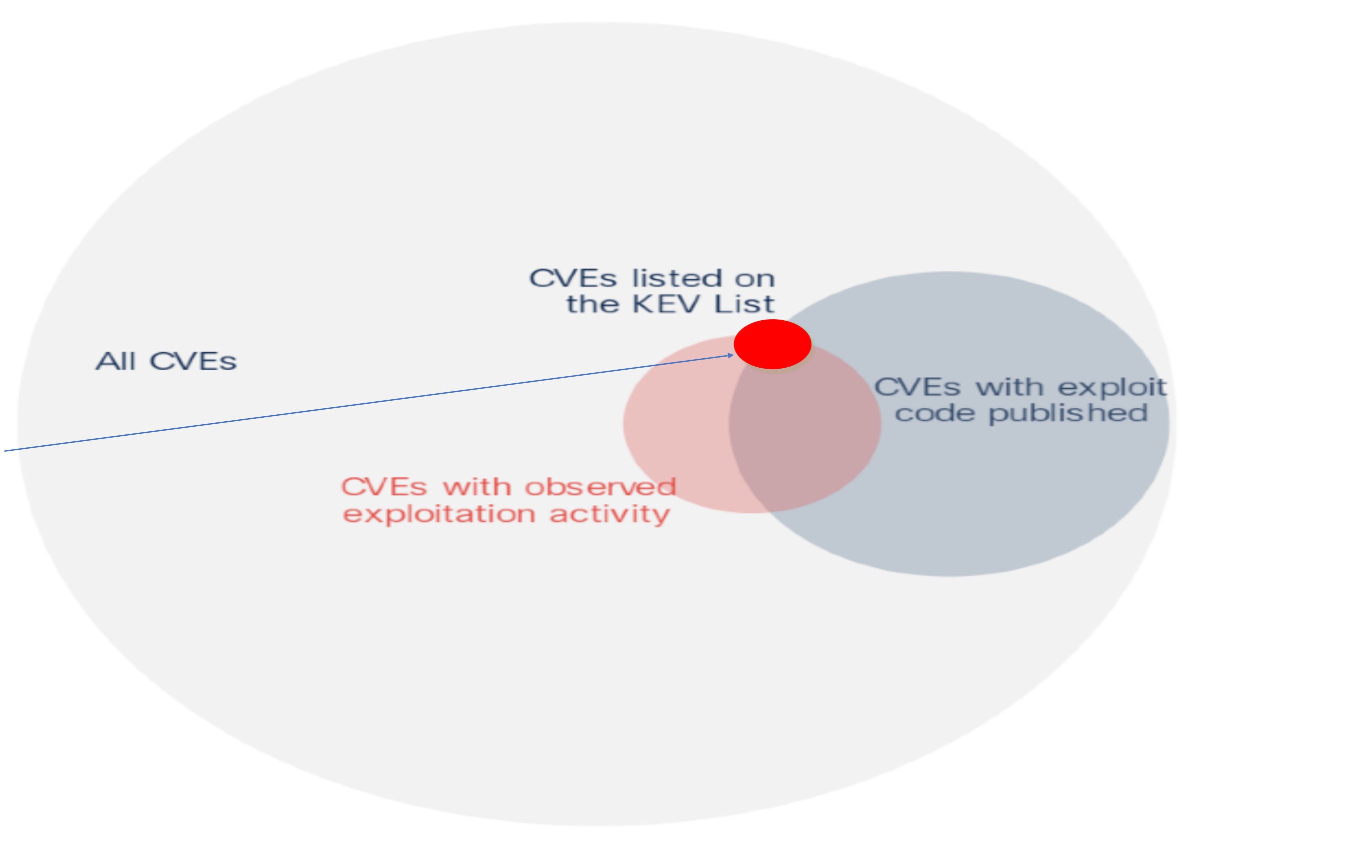
- The increasing number of 0-days used is mostly due to ransomware profits that enable gangs to buy 0-day on the black market in direct competition with states (ransomware more profitable than drugs)

Huge number of vulns but a few one used



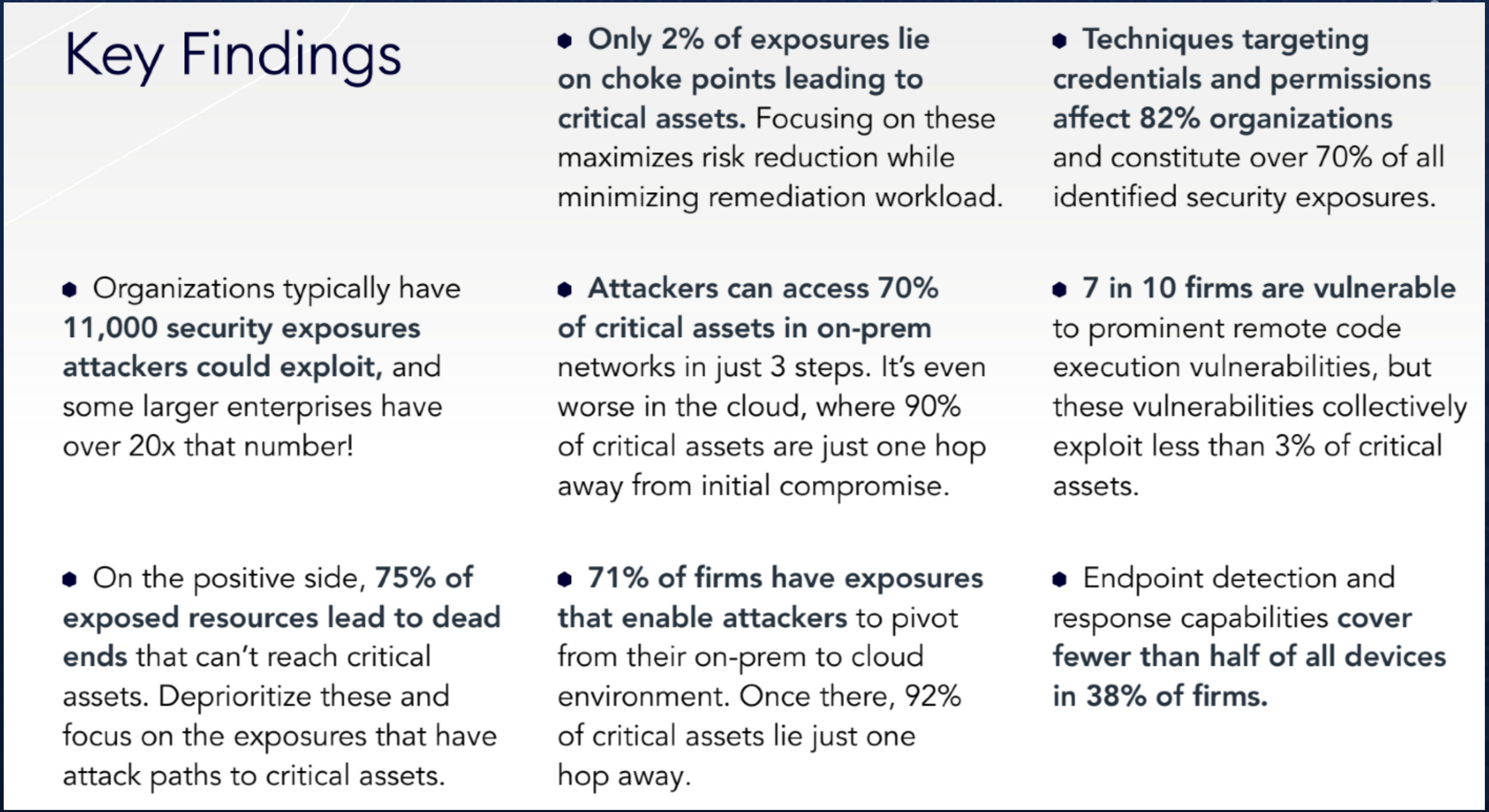
CISA's catalog of must-patch vulnerabilities crosses the 1,000 bug mark after 2 years

The Cybersecurity and Infrastructure Security Agency (CISA) added the 1,000th bug to its Known Exploited Vulnerability catalog this week after nine new issues were spotlighted.


CVEs listed on the KEV List
All CVEs
CVEs with exploit code published
CVEs with observed exploitation activity

Assuming I am willing to patch, which vulnerabilities should I patch since most vulnerability scoring systems are inconsistent?

Large number of exposures



Key Findings

- **Only 2% of exposures lie on choke points leading to critical assets.** Focusing on these maximizes risk reduction while minimizing remediation workload.
- **Techniques targeting credentials and permissions affect 82% organizations** and constitute over 70% of all identified security exposures.
- Organizations typically have **11,000 security exposures attackers could exploit,** and some larger enterprises have over 20x that number!
- **Attackers can access 70% of critical assets in on-prem** networks in just 3 steps. It's even worse in the cloud, where 90% of critical assets are just one hop away from initial compromise.
- **7 in 10 firms are vulnerable** to prominent remote code execution vulnerabilities, but these vulnerabilities collectively exploit less than 3% of critical assets.
- On the positive side, **75% of exposed resources lead to dead ends** that can't reach critical assets. Deprioritize these and focus on the exposures that have attack paths to critical assets.
- **71% of firms have exposures that enable attackers** to pivot from their on-prem to cloud environment. Once there, 92% of critical assets lie just one hop away.
- Endpoint detection and response capabilities **cover fewer than half of all devices in 38% of firms.**

Where defenders see vulnerabilities, the attackers see attack path

A quantitative approach to replace fear, uncertainty and doubts (McKinsey 2023)

A scheduling of countermeasures exists that guarantees
the best return AND the smallest investment

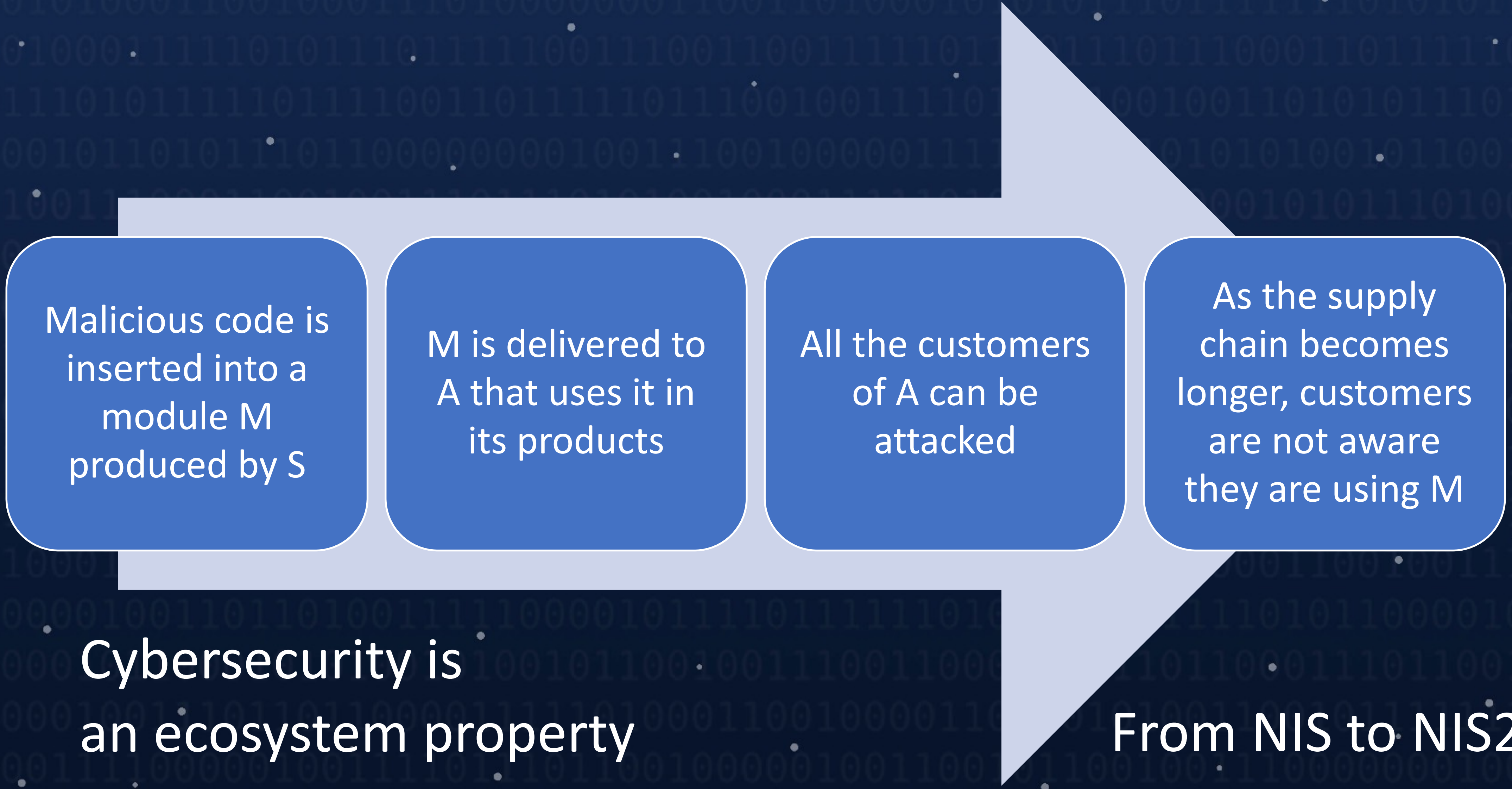
To build the best countermeasure scheduling
we need to know all the attack paths

=

The discovery of all the attack paths
needs formal and executable models
rather than penetration tests or vulnerability assessments

Current & future challenge

Supply chain attacks



Malicious code is inserted into a module M produced by S

M is delivered to A that uses it in its products

All the customers of A can be attacked

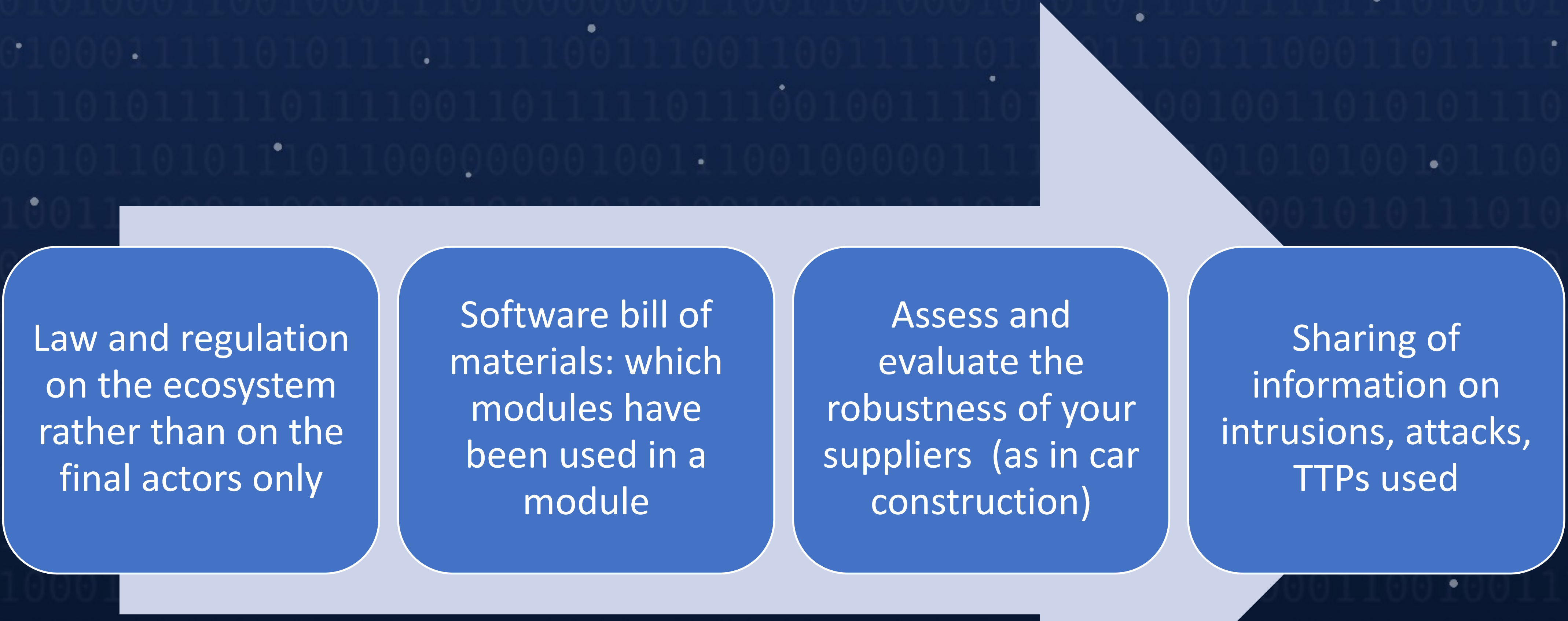
As the supply chain becomes longer, customers are not aware they are using M

Cybersecurity is
an ecosystem property

Supply chain attacks

1.	June 2023	–	MOVEit
2.	March 2023	–	3CX
3.	February 2023	–	Applied Materials
4.	December 2022	–	PyTorch Framework
5.	December 2022	–	Fantasy Wiper
	.....		
n.	July 2021	–	Kaseya
n+k .	April 2021	–	CodeCov
n+k+j	December 2020	–	SolarWinds

Supply chain attacks: defense



Law and regulation on the ecosystem rather than on the final actors only

Software bill of materials: which modules have been used in a module

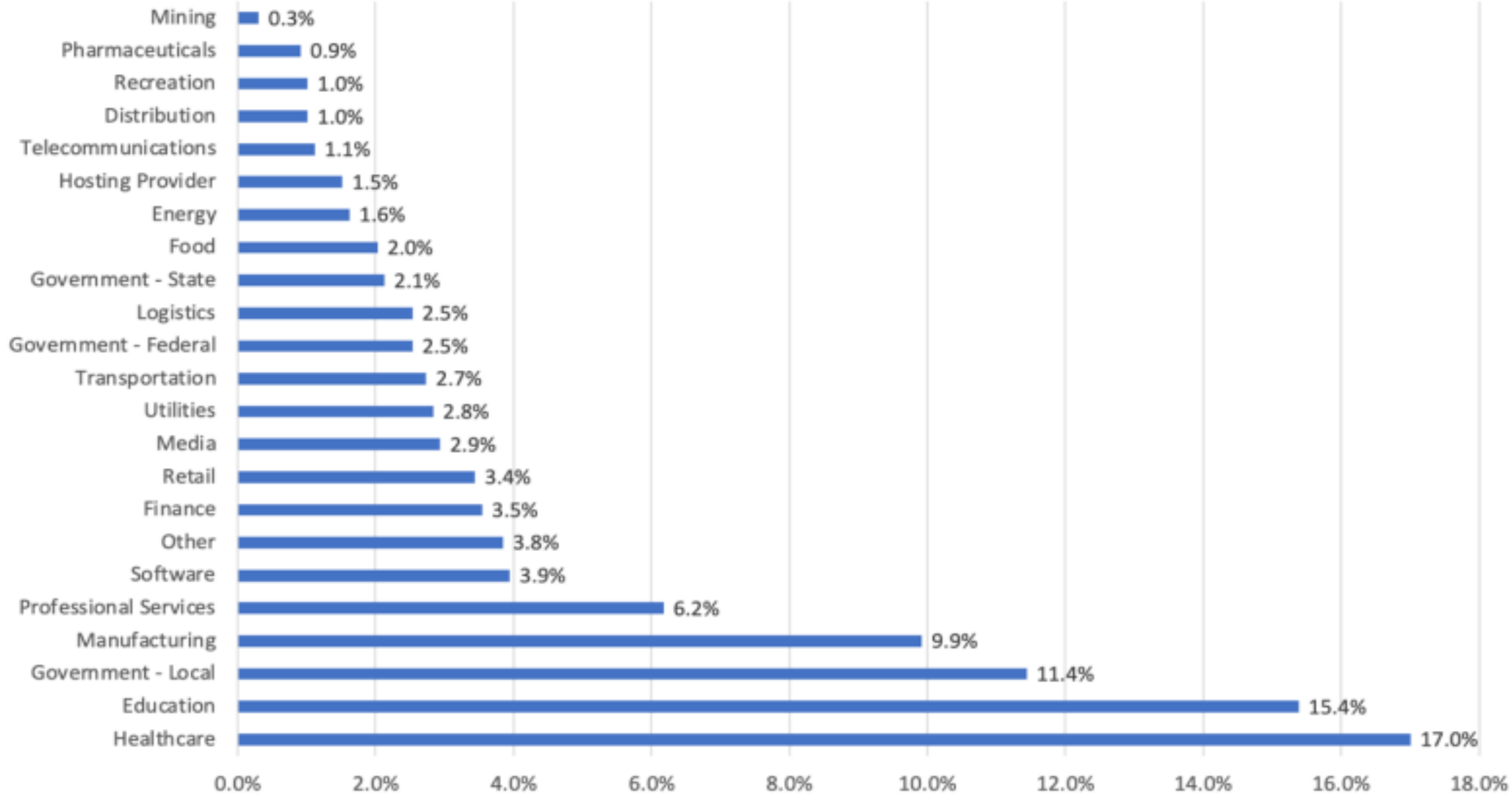
Assess and evaluate the robustness of your suppliers (as in car construction)

Sharing of information on intrusions, attacks, TTPs used

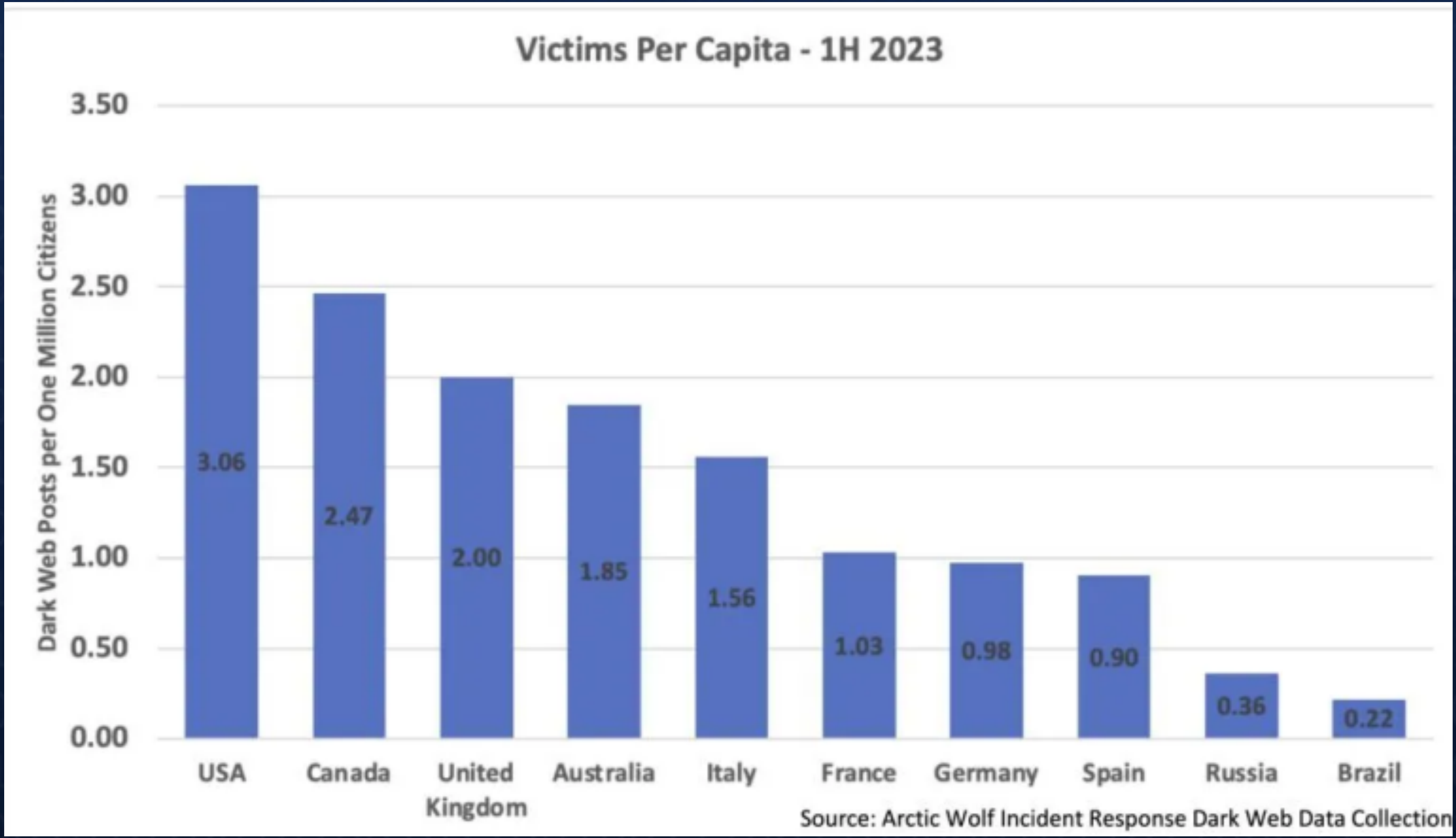
SBOM to be adopted even by open source projects

Ransomware

Distribution of Destructive Ransomware Events by Industry Sector



Ransomware



Source: Arctic Wolf Incident Response Dark Web Data Collection

Italy is the winner after English-speaking countries

Ransomware

- The most interesting feature is not technical but is related to the whole ecosystem = RaaS, ransomware as a service
- A ransomware intrusion involves several gangs
  - Producer of the malware
  - Initial Access
    - Sells access to the target system
  - Ransomware distribution and Service
    - Distributes the malware, offers services to bargain the ransom and help desk to the victims
  - Affiliates
    - Acquires the initial access, chooses the malware, acquires the malware from the distribution, and implements the lateral movements to spread the malware
  - Money laundering
    - Very useful because someone discovered that cryptocurrencies are not anonymous

Ransomware

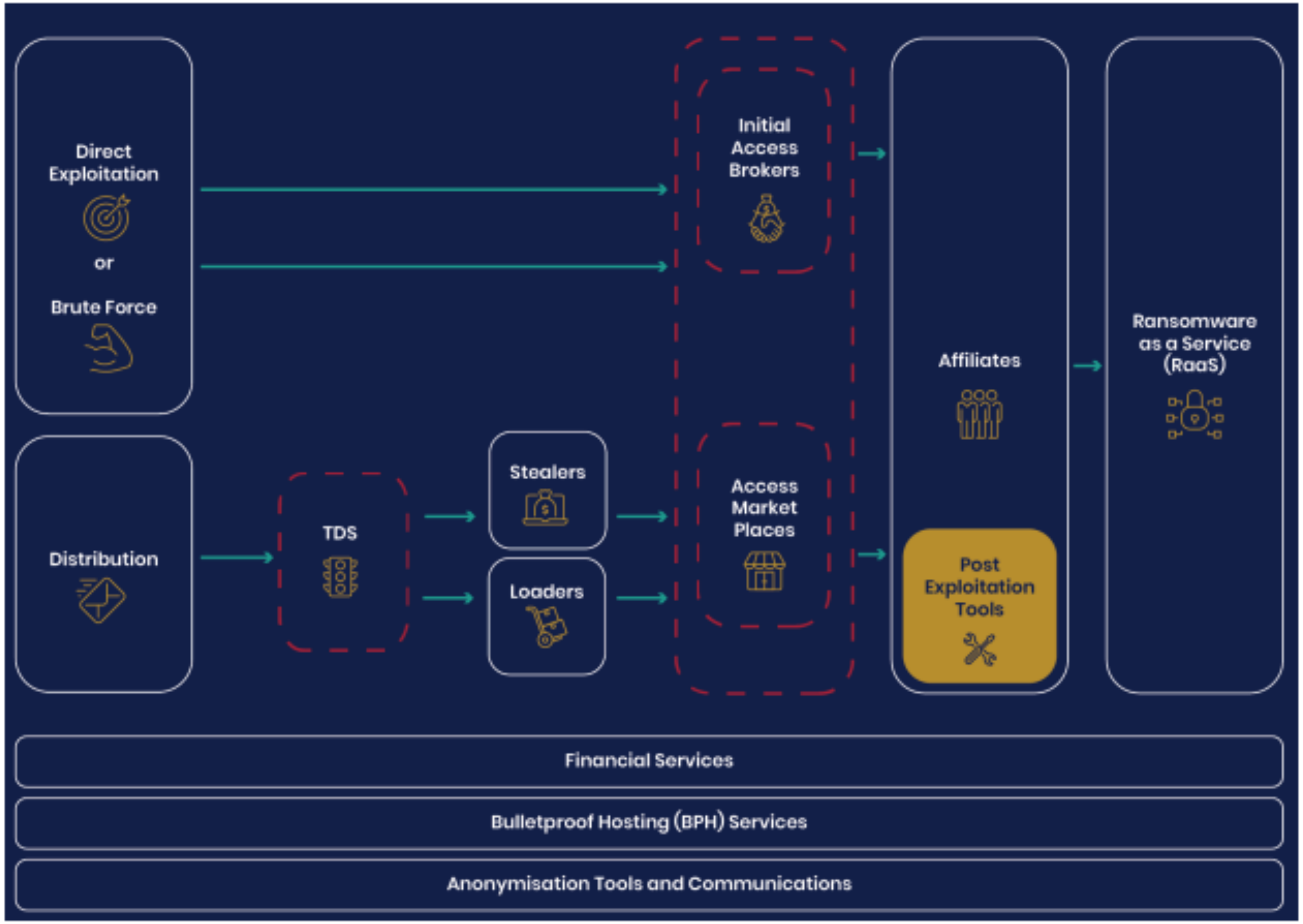
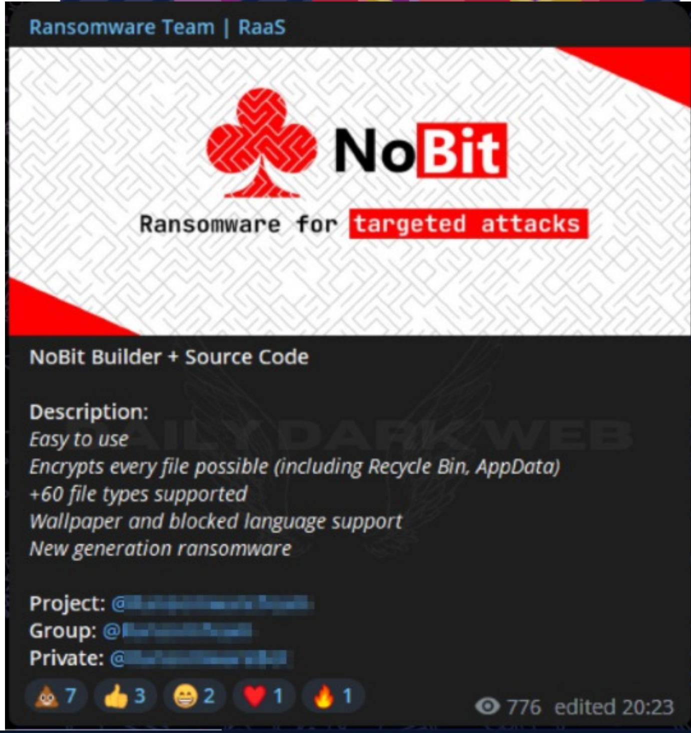


Figure 2. Simplified ransomware workflow

Ransomware, extortion and the cyber crime ecosystem

A white paper from the NCSC and the NCA.



Ransomware Team | RaaS

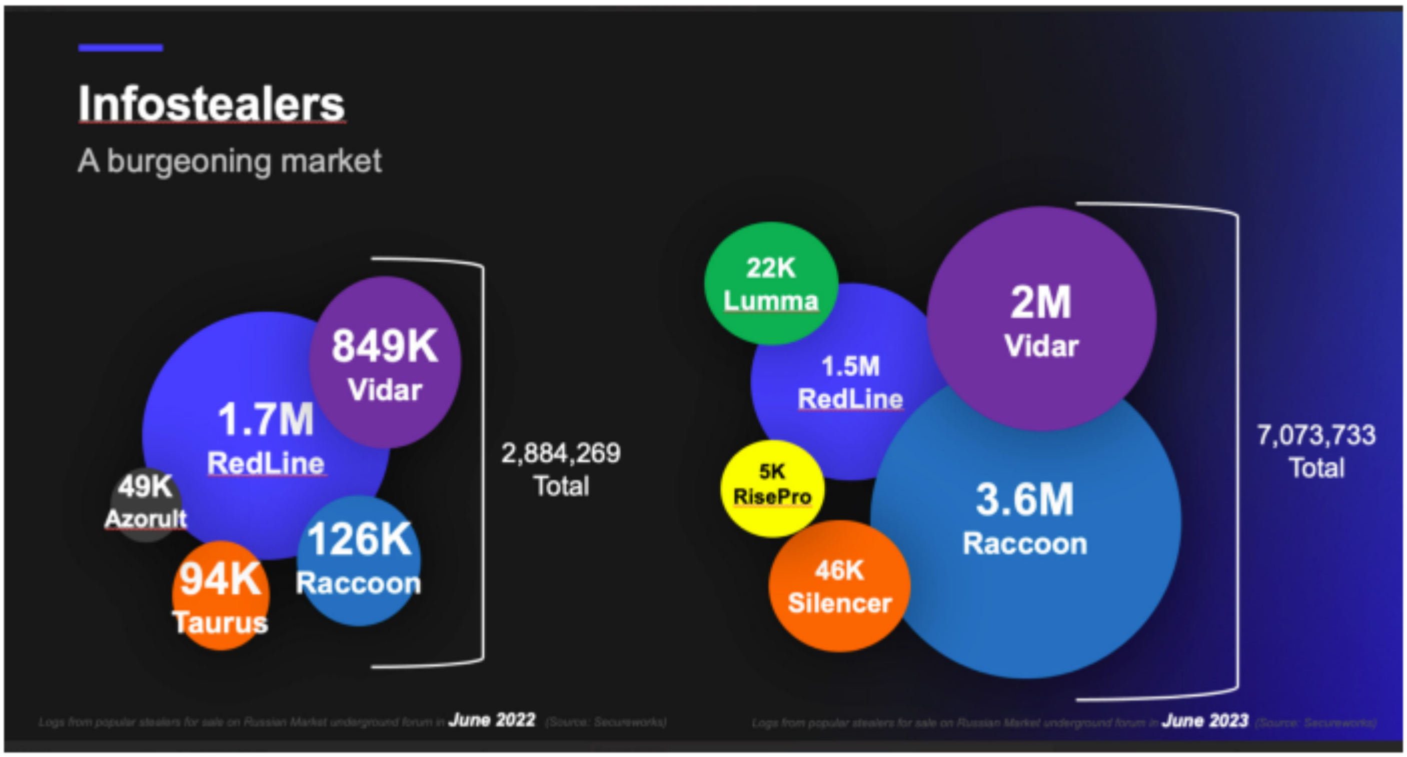
NoBit Builder + Source Code

Description:
Easy to use
Encrypts every file possible (including Recycle Bin, AppData)
+60 file types supported
Wallpaper and blocked language support
New generation ransomware

Project: @[redacted]
Group: @[redacted]
Private: @[redacted]

Ransomware

- Attributing an intrusion to one gang is almost impossible even because there is a continuous exchange among gangs
- A huge amount on access on sale



Infostealers

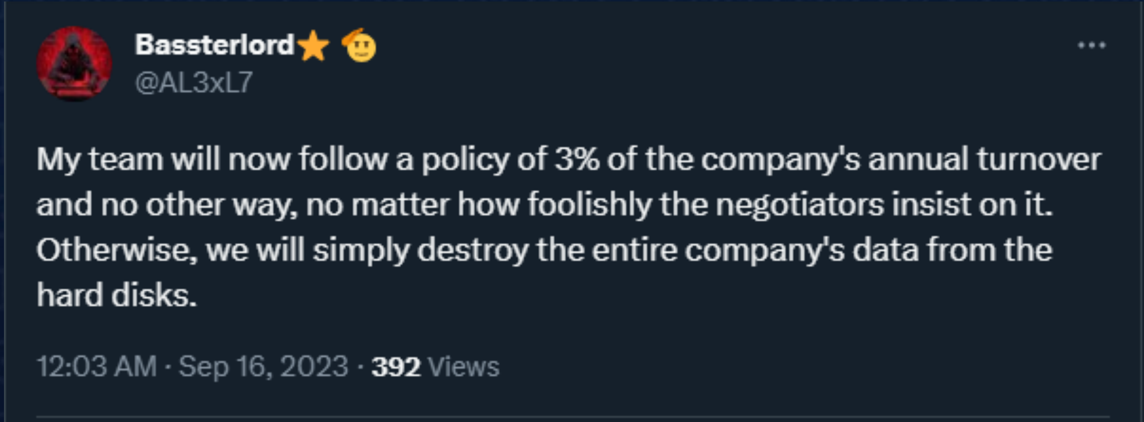
A burgeoning market

Logs from popular stealers for sale on Russian Market underground forum in June 2022 (Source: Secureworks)

Logs from popular stealers for sale on Russian Market underground forum in June 2023 (Source: Secureworks)

Ransomware –Lockbit new rules for affiliates

- Lockbit is considering new affiliate rules due to frustration with negotiators.
- Currently, no rules in place for how much (or how little) affiliates can ransom a company for. Newer affiliates are giving large discounts to victim out of desperation for money, whereas more experienced affiliates do not cave to negotiator's proposed payment from the victims.
- Lockbit administrative staff are proposing a poll with the following options.
  - No changes in payment policy, payment options will remain"unregulated" and remain up to the affiliates.
  - The minimum payment allowed to be 3% of the victim companies annual revenue with the option affiliates can only grant a 50% discount of the original ransom.
  - No payment below the maximum insurance of the victim.
  - A minimum payment of 50% of the insurance.



Bassterlord
@AL3xL7

My team will now follow a policy of 3% of the company's annual turnover and no other way, no matter how foolishly the negotiators insist on it. Otherwise, we will simply destroy the entire company's data from the hard disks.

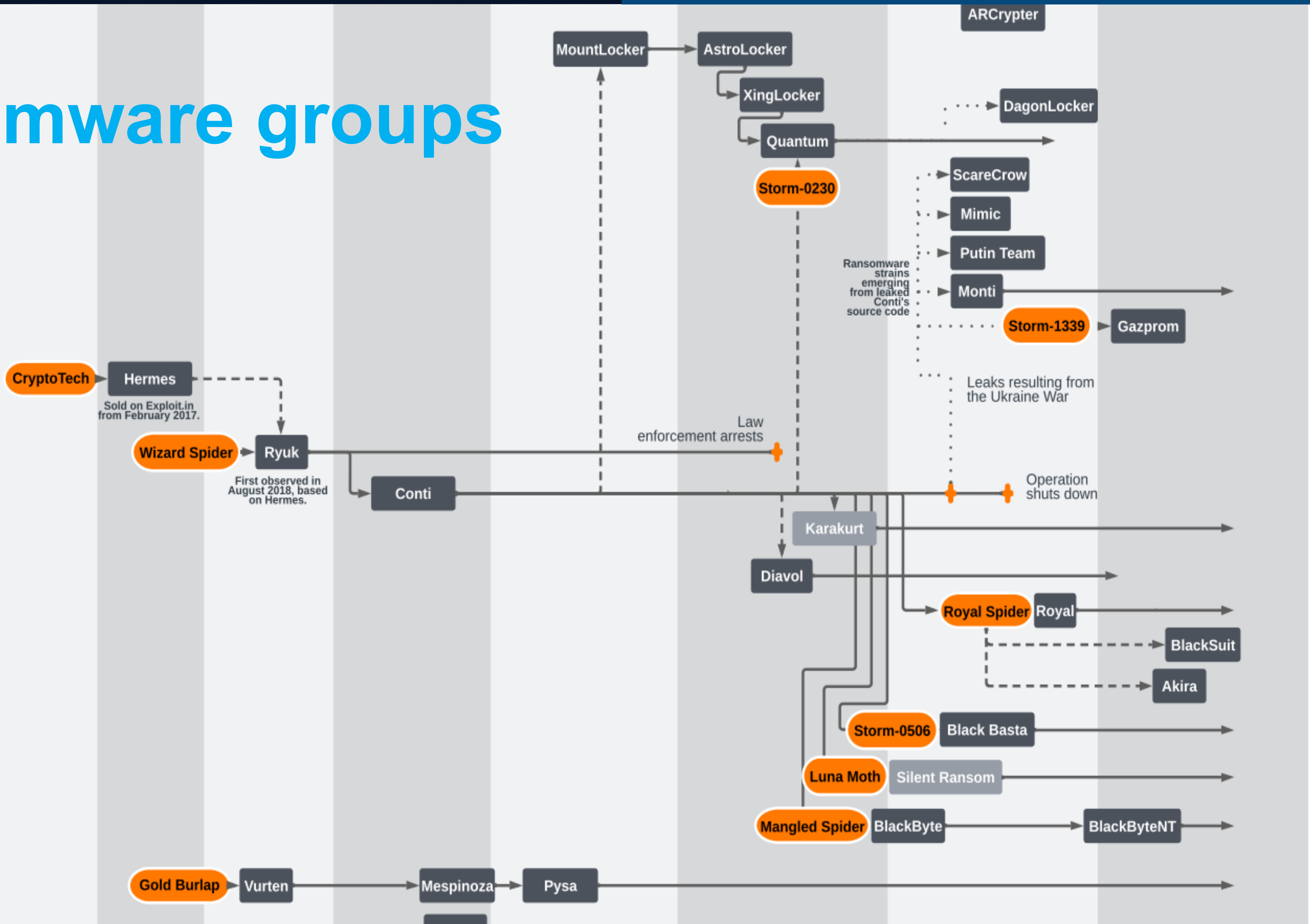
12:03 AM · Sep 16, 2023 · 392 Views

Ransomware groups

Haruspex

Università di Pisa

Ransomware groups
Conti



Ransomware defense

- Robustness, backup even immutable ones are useless against double, triple extortion and quadruple extortion
- Hygiene to remove botnets used as attack infrastructure
- Resilience for business continuity
- A final solution requires an answer to a very complex question

  «is ransomware an act of proxy war?»

  - No ransomware attack has been reported in Russian speaking country (best defense is connecting a russian keyboard)
  - Frequency of attacks in a country increases with political deadlines
  - Some authors speak of **letters of marque** like pirates in XVI century

Ransomware letters of marque

Microsoft Threat Intelligence

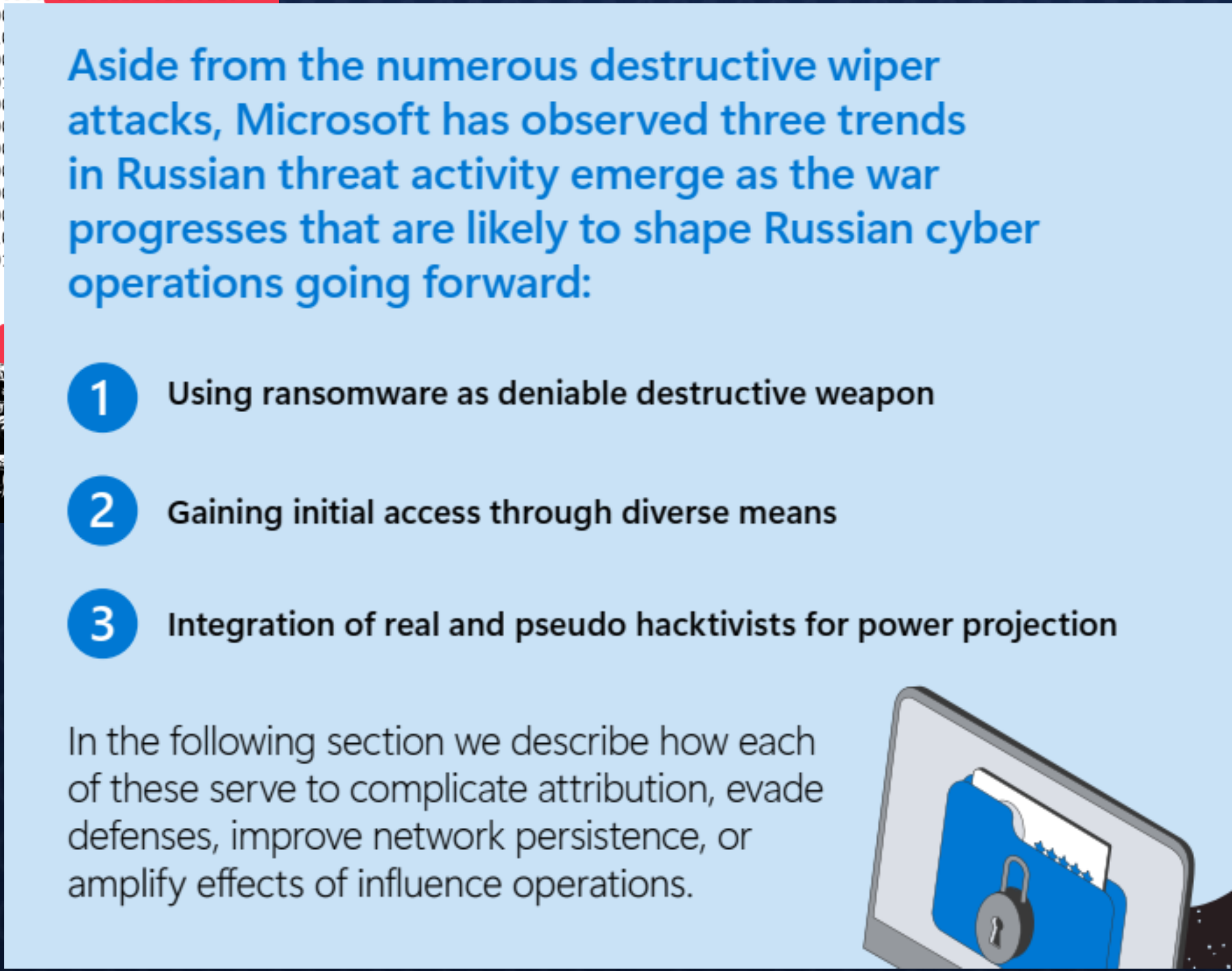
A year of Russian hybrid warfare in Ukraine

What we have learned about nation state tactics so far and what may be on the horizon

March 15, 2023

Microsoft

01000001 00100000 01111001
01100101 01100001 01110010
00100000 01101111 01100110



Aside from the numerous destructive wiper attacks, Microsoft has observed three trends in Russian threat activity emerge as the war progresses that are likely to shape Russian cyber operations going forward:

1. Using ransomware as deniable destructive weapon
2. Gaining initial access through diverse means
3. Integration of real and pseudo hacktivists for power projection

In the following section we describe how each of these serve to complicate attribution, evade defenses, improve network persistence, or amplify effects of influence operations.

Ransomware letters of marque

NUOVA EDIZIONE AGGIORNATA

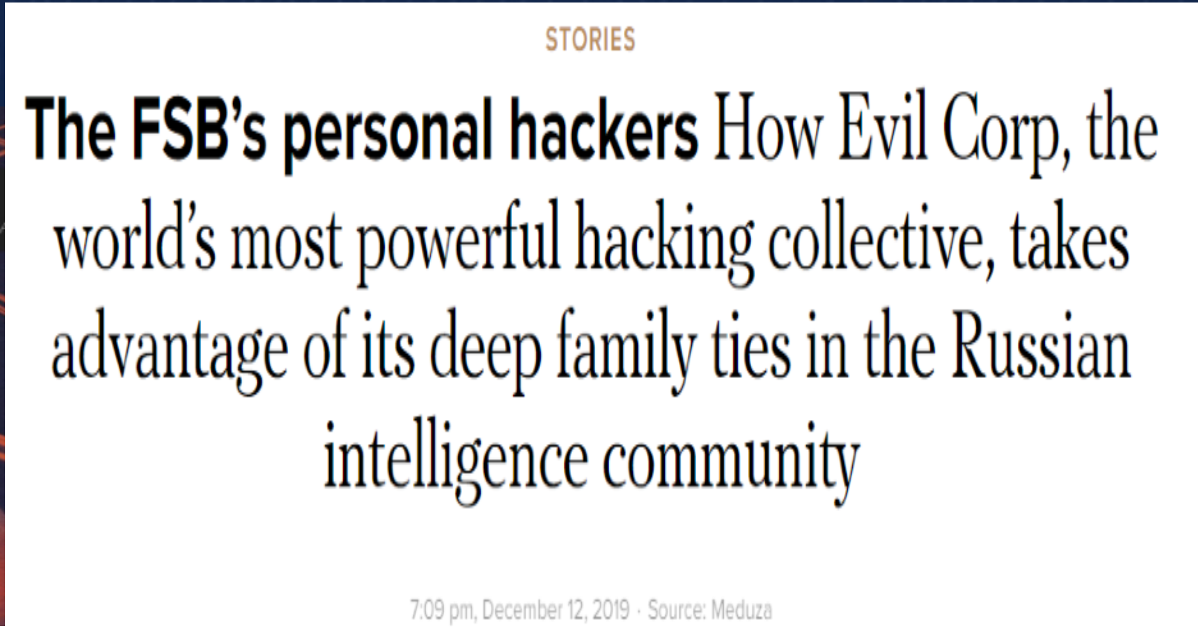
Marta F. Ottaviani

Brigate russe

LA GUERRA OCCULTA DEL CREMLINO CONTRO L'OCCIDENTE

BOMPIANI MUNIZIONI

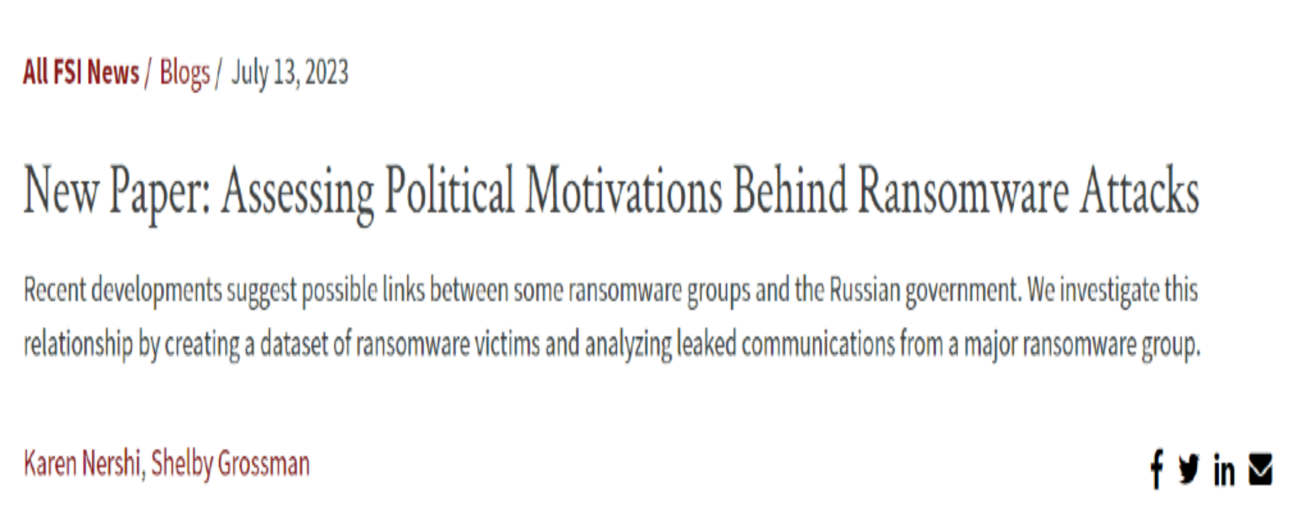
COLLANA DIRETTA DA ROBERTO SAVIANO



STORIES

The FSB's personal hackers How Evil Corp, the world's most powerful hacking collective, takes advantage of its deep family ties in the Russian intelligence community

7:09 pm, December 12, 2019 · Source: Meduza



All FSI News / Blogs / July 13, 2023

New Paper: Assessing Political Motivations Behind Ransomware Attacks

Recent developments suggest possible links between some ransomware groups and the Russian government. We investigate this relationship by creating a dataset of ransomware victims and analyzing leaked communications from a major ransomware group.

Karen Nershi, Shelby Grossman

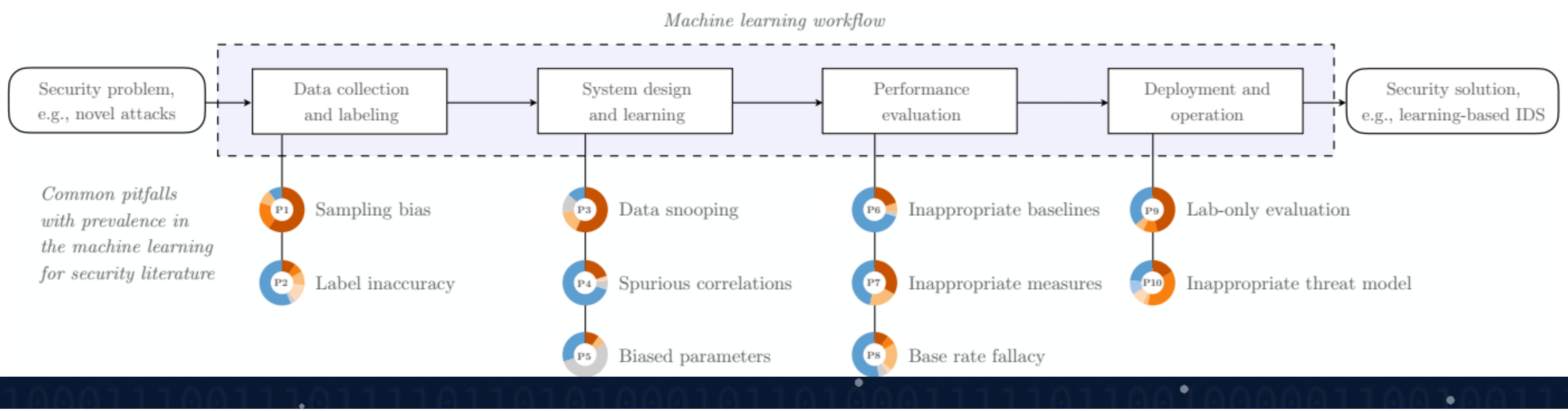
AI and Cybersecurity

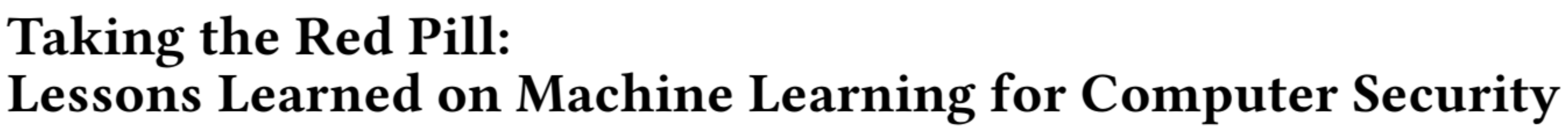
Most researchers had great expectations on the cybersec fields where the recent huge development in AI can impact

- Better phishing letters in any language
- Vulnerability discovery by static analysis of program code
- Attack detection
- Decision support in an intrusion

Vulnerability discovery & attack detection

- Spurious results

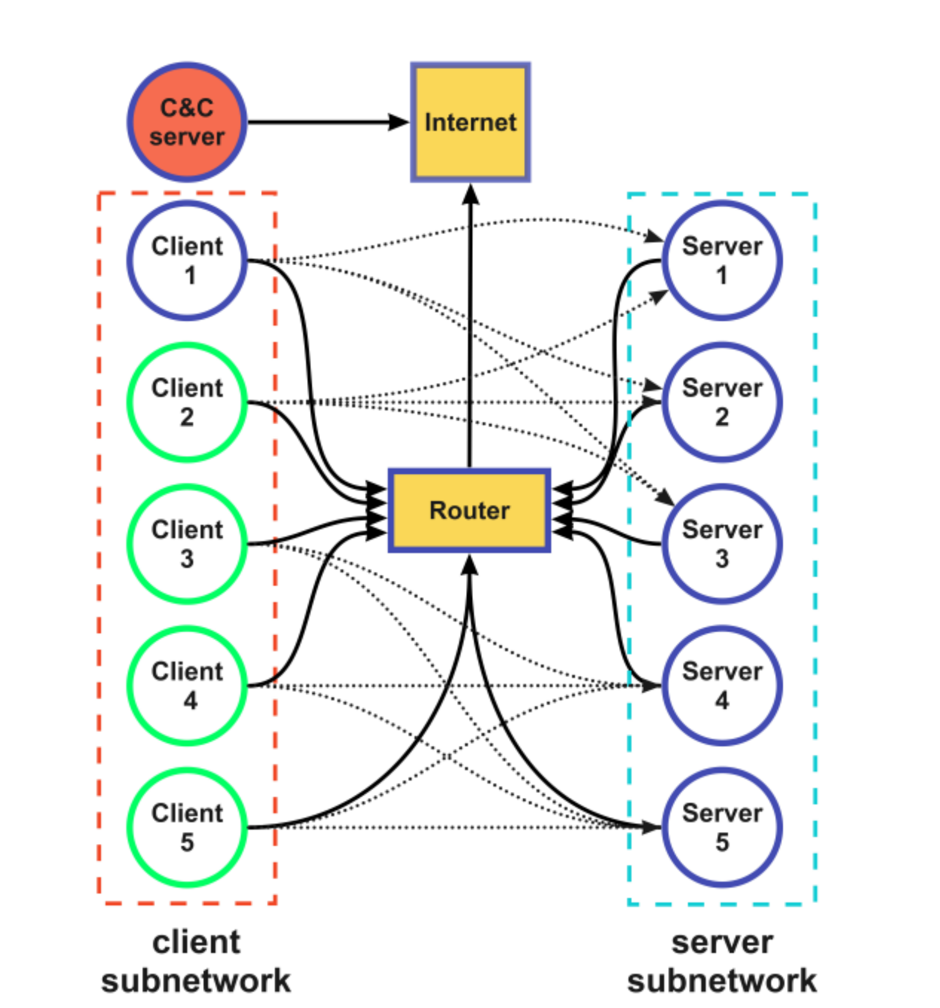

Machine learning workflow
Security problem, e.g., novel attacks
Data collection and labeling
System design and learning
Performance evaluation
Deployment and operation
Security solution, e.g., learning-based IDS
Common pitfalls with prevalence in the machine learning for security literature
P1
Sampling bias
P2
Label inaccuracy
P3
Data snooping
P4
Spurious correlations
P5
Biased parameters
P6
Inappropriate baselines
P7
Inappropriate measures
P8
Base rate fallacy
P9
Lab-only evaluation
P10
Inappropriate threat model

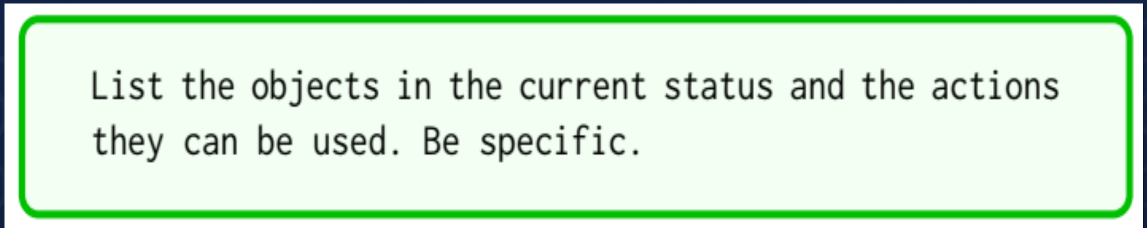


Taking the Red Pill:
Lessons Learned on Machine Learning for Computer Security

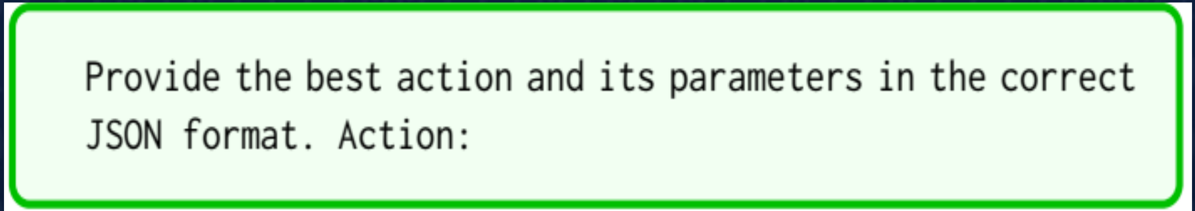
Decision Support

Out of the Cage: How Stochastic Parrots Win in Cyber Security Environments

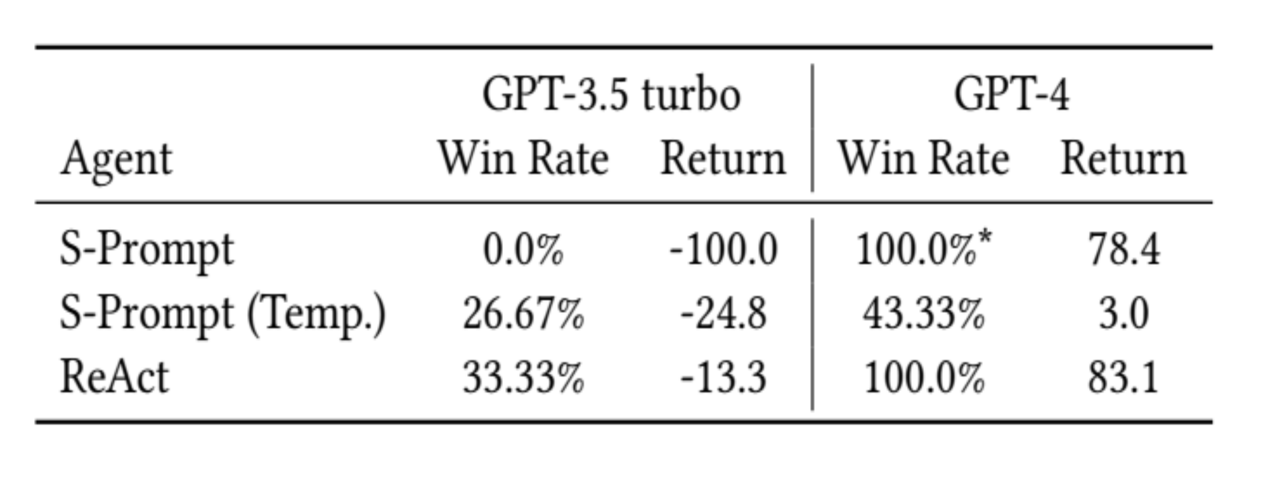




```
List the objects in the current status and the actions
they can be used. Be specific.
```



```
Provide the best action and its parameters in the correct
JSON format. Action:
```



	GPT-3.5 turbo		GPT-4	
Agent	Win Rate	Return	Win Rate	Return
S-Prompt	0.0%	-100.0	100.0%*	78.4
S-Prompt (Temp.)	26.67%	-24.8	43.33%	3.0
ReAct	33.33%	-13.3	100.0%	83.1

Decision Support

Problems

- Allucinations: LLMs had the tendency to propose actions using objects that were not described in the current state
- Invalid or repeated actions
- Cost*:* The GPT-4 API is quite expensive and 30x more expensive than GPT-3.5
- Instability: Fine tuning may create reproducibility issues
- Prompt creation: A change in the word order in a query may have a disruptive impact on the result
- Learning: Not clear how to describe a state

Decision Support

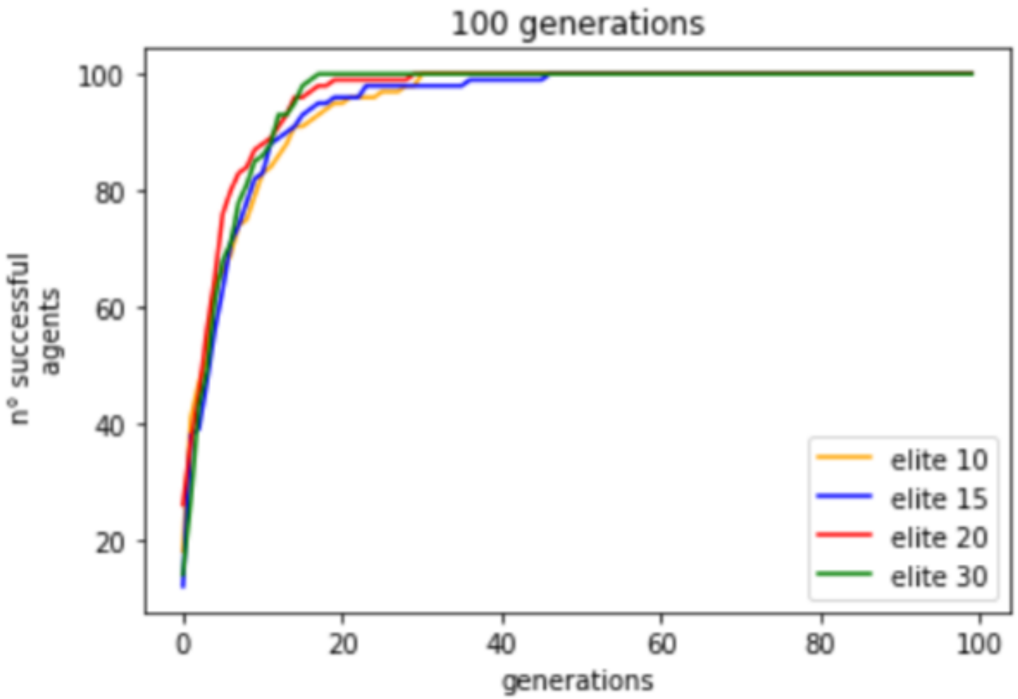
Discovering How to Attack a System

F. Baiardi, D. Maggi, M. Passacantando

Learning how to attack a system is possible

Much harder to generalize what has been learn to attack any system

Transfer learning not obvious



AI & cybersecurity: an old story

- Several attacks are possible against AI systems
  - Adversarial attacks
  - Poisoning of training data
  - ....

- Discovering some of these attacks is almost impossible after the training

- Just a few are worried by these
- problems maybe because they will take care of them in the next versio

Cybersecurity Action Team

Securing AI: Similar or Different?

Anton Chuvakin, John Stone, Tanya Popova-Jones at Office of the CISO, Google Cloud

Securing AI: Similar or Different?

There are many ways AI systems can be vulnerable to attack. For example, AI systems can be tricked into making incorrect decisions by feeding them malicious data. Additionally, AI systems can be hacked to gain access to sensitive data or to take control of the system itself. Attacks on AI systems can impact the security of the system, but could also cause harm or privacy issues. It’s therefore essential to take steps to secure AI systems. This includes ensuring that AI systems are fully part of cyber governance, that they’re protected from malicious attacks, and that their security is regularly reviewed. In addition to securing AI systems, it’s also important to ensure that AI is used in a secure way, as even the securely developed platform may be used in a less secure manner (public cloud being a great example here)

Haruspex
Cyber Risk Assessment and Management

Thanks to Luca for the invitation
and to you for listening
Waiting for your questions
Hope to be able to answer …